

National Credit Union Administration



National Association of Federal Credit Unions

Information Systems & Technology Audio Conference

Arlington, VA

October 4, 2000

**NAFCU Audio Conference
10/04/2000
NCUA Information Systems & Technology (IS&T)**

- 1) IS&T Initiatives
 - a) NCUA Strategic Goal #2
 - i) "Ensure that credit unions are prepared to safely integrate financial services and emerging technology in order to meet the changing needs of their members."
 - b) Outcome Goal 2.1
 - i) Ensuring access to information and training about financial technology services.
 - c) Outcome Goal 2.2
 - i) Understanding and dealing with emerging security threats.
 - d) Outcome Goal 2.3
 - i) Promoting public trust.
 - e) Do credit unions have to develop and implement e-Commerce services?
 - i) NO!
 - ii) NCUA encourages credit unions to consider offering e-Commerce services.
- 2) NCUA Guidance
 - a) Rules & Regulations
 - i) Part 716 Privacy of Consumer Financial Information (Final)
 - ii) Part 741 Privacy of Consumer Financial Information Requirements for Insurance (Final)
 - iii) Part 748 Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance (Proposed; Comments due August 6, 2000)
 - b) Letters To Credit Unions
 - i) 97-CU-5 Interagency Statement on Retail On-line PC Banking
 - c) Regulatory Alerts
 - i) 98-RA-4 Interagency Guidance on Electronic Financial Services and Consumer Compliance
 - d) Other
 - i) FFIEC Information Systems Examination Handbook
- 3) Applicable Laws & Regulations
 - a) Electronic Funds Transfer Act
 - b) Equal Credit Opportunity Act
 - c) Expedited Funds Availability Act
 - d) Fair Credit Reporting Act
 - e) Fair Housing Act
 - f) Real Estate Settlement and Procedures Act
 - g) Right to Financial Privacy
 - h) Reserve Requirements for Depository Institutions
 - i) Truth in Lending Act
 - j) Truth in Savings Act
 - k) Equal Employment Opportunity Act
 - l) Consumer Leasing Act
 - m) Home Mortgage Disclosure Act
 - n) Others???
- 4) Federal Legislation Specific to e-Commerce:
 - a) Child On-Line Privacy Protection Act (COPPA)
 - b) Gramm-Leach-Bliley Act
 - c) Rules & Regulations Part 716
 - d) Rules & Regulations Part 748
 - e) Electronic Signatures in Global and National Commerce Act (E-Sign)
- 5) Information Systems & Technology Examination Program (ISTEP)
 - a) Risk-Based Focus

- b) Evaluate Management Oversight
 - i) Identify Risks
 - ii) Assess Risks
 - iii) Measure Risks
 - iv) Mitigate Risks
 - v) Monitor Risks
 - c) Risk Categories (Typical)
 - i) Operational/Transactional
 - ii) Compliance
 - iii) Strategic
 - iv) Reputational
 - d) Examination Tools:
 - i) e-Commerce I (EC-1)
 - ii) e-Commerce II (EC-2)
 - iii) Electronic Data Processing Review (EDPR)
- 6) Electronic Financial Services (EFS)
- a) Electronic Payment Systems
 - i) ACH Transactions
 - ii) Stored Value Cards
 - iii) Electronic Money
 - iv) Electronic Wallets
 - v) ATM Systems
- 7) Electronic Commerce (e-Commerce) **Systems**
- a) Website Systems (Internet/Browser based)
 - b) Home Banking (PC based)
 - c) Audio Response (Phone based)
 - d) Wireless
 - e) Kiosk
- 8) Electronic Commerce (e-Commerce) **Services**
- a) Internet/World Wide Web Services
 - b) Home Banking Services
 - c) Online Bill Paying Services
 - d) Account Transaction Services
- 9) Credit Union IS&T Reviews
- a) Safety & Soundness Examiners
 - i) High level review
 - ii) Scope based upon Examiner judgment
 - iii) Part of annual examination
 - b) Information Systems Officers
 - i) In-depth review
 - ii) Flexible scope
 - iii) Part of, or in addition to, annual examination
 - c) IS&T CAMEL Rating Impact
 - i) Management Component
 - (1) Evaluation Criteria
 - (a) Strategic Plan & Goals
 - (b) Risk Analysis
 - (c) Policies/Procedures
 - (d) Oversight
 - (2) Other components if applicable

- 10) NCUA Vendor Reviews
 - a) Approximately 2 - 3 reviews YTD
 - b) Year 2001
 - i) Proposing 10 - 20 reviews
 - c) Report Distribution
 - i) NCUA distributes the report to the client credit unions of the vendor
 - ii) NCUA distributes report to FFIEC agencies, if applicable
- 11) FFIEC Vendor Reviews
 - a) Typical Report Categories:
 - i) Multi-Regional Data Processing Services (MDPS)
 - ii) Shared Application Software Review (SASR)
 - iii) Independent Data Center (IDC)
 - b) Report Distribution:
 - i) Each agency distributes the report to the client institutions of the vendor for institutions the agency regulates.
- 12) Other Issues
 - a) SAS70 & SAS65 Reports
 - i) Determine if a report exists
 - ii) Determine whether to request a copy
 - iii) If obtained, review and mitigate identified risks
 - b) Security Issues
 - i) Penetration Tests vs. Risk Analysis
 - ii) Intrusion Detection (real-time???)
 - c) Consistent Application of Guidance
 - i) Guidance issued by the Central Office is the minimum standard.
 - ii) Each region is different and must have the flexibility to deal with conditions and issues unique to their region.
 - iii) Each credit union is unique and different.

Discussion

Introduction

First of all, I would like to take this opportunity to thank NAFCU for asking us to come speak to you today and to thank you for participating in this discussion. One of NCUA's strategic goals, which we will discuss shortly, deals with the sharing information with the credit union community. Forums like this audio conference, provide us the opportunity to meet that goal.

There are a wide range of issues and items that I would like to discuss today; however, our time is limited so I would like to focus on those areas which I believe are of most interest. I believe each of you have a copy of the extended agenda, so if I don't discuss something contained in the agenda and you have a question about it, please feel free to bring it up during our Q&A session. It is also important for us to receive feedback from you concerning NCUA's Information Systems & Technology Examination Program. Your feedback, ideas, and concerns will help us refine the program and make it more beneficial to you and NCUA.

Also, please keep in mind that many of the items we will discuss today are subject to change, and probably will change. As we develop and implement the various examination programs we will talk about today, we will revise and tweak them to meet the changing information systems and technology environment. As I stated earlier, it is important to receive feedback, from credit unions, examiners, and trade associations in order to provide the best examination tools to our staff and which are beneficial to you.

The key items I would like to discuss today are:

- IS&T Initiatives;
- NCUA's Information Systems & Technology Examination Program (ISTEP);
- Credit Union IS&T Reviews;
- Vendor Reviews:
 - NCUA

- FFIEC; and
- Security Issues

IS&T Initiatives

NCUA's IS&T initiatives are being driven by our Strategic Plan (for the years 2000 – 2005) and the economic and dynamically changing market place that credit unions must compete within. In particular, Strategic Goal #2 deals with information systems and technology and reads as follows:

“Ensure that credit unions are prepared to safely integrate financial services and emerging technology in order to meet the changing needs of their members.”

There are some key terms in that statement that I would like to highlight for you. These terms are:

- safely integrate;
- emerging technology; and
- changing needs.

These key terms go to the heart of what NCUA's IS&T initiatives are all about...ensuring the safety and soundness of credit unions while employing new technologies to provide additional, or enhance existing, services to meet the changing needs of their membership.

In order to meet this strategic goal, we have broken the goal down into three major outcome goals and then developed strategies to meet these outcome goals.

Outcome Goal 2.1 states:

“Ensure that credit unions have access to information and training about emerging financial service technology and use this information to integrate innovative

technology planning, contracting, deployment, and support within the credit union format.”

Our strategies for Outcome Goal 2.1 are:

- Improve NCUA staff understanding of technology to enhance financial service products and member services and operations.
- Develop methodologies (such as web pages) for sharing information, best practices, and resources with examiners and credit unions.
- Ensure technology training is adequate, effective, and available.
- Encourage credit union mentoring and partnerships arrangements to share best practices, resources, and other information (similar to the small credit union program implemented several years ago).
- Encourage credit unions to develop technology plans.

Outcome Goal 2.2 states:

“Ensure that credit unions understand emerging security threats and are prepared to deal with them.”

Our strategies for Outcome Goal 2.2 are:

- Develop IT control guidelines for credit unions.
- Assess the adequacy of credit union security and internal controls both individually and the industry as a whole.
- Work with the Federal Financial Institutions Examination Council (FFIEC) to conduct research and analysis to understand emerging security threats.
- Work with law enforcement agencies to understand the nature of emerging threats and vulnerabilities and coordinate with the FFIEC agencies to develop common approaches to dealing with security threats.
- Develop a system for communicating threats, issues, and vulnerabilities to credit unions.

Outcome Goal 2.3 states:

“Promote public trust in credit union deployment of emerging technology.”

Our strategies for Outcome Goal 2.3 are:

- Seek permanent supervisory authority over credit union service providers.
 - The Examination Parity and Year 2000 Readiness Act for Financial Institutions (also referred to as Exam Parity Act), enacted on March 20, 1998 provides the authority for NCUA and OTS to conduct examinations of vendors and service providers. This Act extends to NCUA and OTS the same examination authority that the other regulators (FDIC, OCC, and FRB) have.
 - However, the Exam Parity Act contains a Sunset Provision in regards to NCUA’s vendor examination authority. NCUA’s authority expires on December 31, 2001. Without this authority, NCUA loses its vendor examination authority and may not be able to share information we obtain about your vendors with you. Expiration of this authority places NCUA on unequal authority in regards to the other financial institutions regulators.
 - Examination & Insurance, as well as the GAO, believe the loss of this authority puts NCUA, and the credit union industry, at a distinct disadvantage. The GAO has recommended that Congress eliminate the Sunset Provision and Examination & Insurance supports that recommendation. There is much to be gained, such as public confidence, by retaining the authority, and much to be lost if the authority is allowed to expire.

Additional strategies for Outcome Goal 2.3 include:

- Acquire the expertise to guide and evaluate credit union e-Commerce programs and services.
- Develop a comprehensive and detailed examination program to evaluate electronic financial services including, but not limited to:
 - security risks;
 - privacy concerns; and

- compliance issues.
- Develop training programs for examiners to keep them abreast of new and emerging electronic financial services and the means by which they will be evaluated.
- Provide training opportunities to specialized corporate examiners who review automated services in corporate credit unions.

The preceding discussion was a high-level review of what Strategic Goal #2 means to NCUA and to credit unions as well as how we plan to implement that goal. We have developed a series of tasks to address each of the strategies previously mentioned; however, in the interest of time, I won't go into those tasks during this discussion.

NCUA's Information Systems & Technology Examination Program (ISTEP)

The next key item I would like to discuss is NCUA's Information Systems & Technology Examination Program (ISTEP). We have split the ISTEP into two primary examination programs: Credit Union Information Systems Examination Program and Vendor Information Systems Examination Program. We further divided each of these two programs into subcategories.

The Credit Union Information Systems Examination Program includes:

- Electronic Financial Services
 - electronic payment systems;
 - ATM/ACH transactions;
 - e-Commerce; and
 - website reviews.
- Electronic Data Processing
 - core processing systems;
 - support processing systems;
 - back-office systems;
 - network communication systems; and
 - router and firewall configurations.

Obviously there are “cross overs” between these two subcategories so they are not mutually exclusive. For example, when reviewing electronic financial services, one can reasonably expect to see routers and firewalls. Therefore, an examiner conducting an electronic financial services review would still include a review of these systems in the EFS review.

The Vendor Information Systems Examination Program includes:

- NCUA conducted Vendor Reviews
 - Primarily focuses on those vendors that provide services to a significant number of credit unions or credit union assets.
 - The process includes reviewing:
 - the management oversight and audit function;
 - systems development and programming;
 - systems security, disaster recovery, and business continuity; and
 - member service.
- FFIEC conducted Vendor Reviews
 - Primarily focuses on those large and complex vendors that provide services to regulated financial institutions.
 - There are 3 primary types of examinations:
 - Multi-regional Data Processing Servicers (MDPS; regional/national servicers who service more than one class of financial institutions);
 - Shared Application Software Reviews (SASR; servicers with turnkey type products/services); and
 - Independent Data Centers (IDC).
 - I mention the types of examinations only because you may receive a copy of the examination report if you are a client of the vendor.

From an examination perspective, the ISTEP is a risk-based focused examination program which evaluates credit union management oversight of the IS&T area. The program will consider whether management had identified, assessed, measured,

mitigated, and monitored the risks associated with the various systems and services used to deliver the products. These risks typically fall into the following categories:

- Operational/Transactional: Risks associated with failure to deliver services or products in the manner intended. This risk is typically inherent in any type of service or product.
- Compliance: Risks associated with failure to comply with laws, rules, regulations, prescribed practices, or ethical standards. This risk also includes failure to comply with established internal policies and procedures.
- Strategic: Risks associated with failure to meet strategic goals due to adverse business decisions or improper decision implementation.
- Reputational: Risks associated with negative public opinion.

There are approximately 5 other risk categories (credit, interest rate, price, liquidity, and foreign exchange); however, the preceding 4 are the ones that are typically associated with IS&T initiatives. As such, our credit union and vendor IS&T reviews generally focus on those 4 primary risk categories.

Credit Union IS&T Reviews

This now leads us into the next key area, Credit Union IS&T Reviews. We have divided these reviews into two examination programs. The first program is part of the safety and soundness examination that your examiner generally conducts each year. The second program, which is proposed, is an IS&T examination focused on information systems and technology. You may recall that I stated earlier that one of the strategies for Outcome Goal 2.3 was to develop a comprehensive detailed examination program to evaluate electronic financial services. This proposed examination process is that program addressing that goal. These type of examinations will typically be led by an IS&T Subject Matter Expert, IS&T Specialist, or Information Systems Officer depending on the complexity of the IS&T systems and/or services provided by the credit union and/or due to an examiner's assessment of IS&T issues or concerns at the credit union.

Safety & Soundness Examinations:

Under the safety & soundness examination program, examiners will assess management's oversight of the IS&T area. This assessment initially focuses on electronic financial services, and more specifically, e-Commerce systems and services. This assessment will be part of, or included in, the examination report you are accustomed to receiving. The tools by which our examiners will use to make their assessment of management oversight are two e-Commerce questionnaires, commonly called EC-1 and EC-2, and an Electronic Data Processing Review program, commonly referred to as EDPR. We delivered these tools to our staff at the regional conferences this year and provided them training on IS&T issues as well as how to use these tools during your examination. If your credit union provides e-Commerce services, you should expect to see your examiner use one or both e-Commerce tools as part of their safety & soundness examination. As a note, examiners may elect to use the Electronic Data Processing Review program whether or not you provide e-Commerce services. The EDPR is a high-level review of your core processing and support systems, is not limited to electronic financial services, and is applicable if you process data electronically. This review program is not required – it is an optional process and the examiner will determine whether to employ the process based upon the scope of the examination and examiner judgement.

IS&T Examinations:

On the other hand, IS&T Examinations are focused specifically on the IS&T area. These examinations may be performed concurrently with the safety & soundness examination or they may be performed as a separate contact. Ideally, your examiner would be knowledgeable of your IS&T initiatives and would be able to determine whether or not to request an IS&T examination and then to coordinate performing both the safety & soundness and IS&T examinations at the same time. However, there could be, and probably will be, those instances where IS&T issues are not known prior to the safety & soundness examination, in which case, a separate contact to perform an IS&T examination would be required.

Report Format(s) and CAMEL Rating:

By now, you are probably wondering what the examination report will look like and how will the IS&T review impact your CAMEL rating. Where the examiner just performs a safety & soundness IS&T review, or when an IS&T examination is performed in conjunction with the safety & soundness examination, your examination report should not change significantly, and possibly none at all. The report structure (overview, document of resolution, examiner findings, etc.) would remain the same (in other words, IS&T issues/concerns would be incorporated into the current format within AIREs). When an IS&T examination is performed outside the safety & soundness examination, we would issue a separate IS&T examination report. We would consider this report to be part of, or an addition to, your safety & soundness examination.

Regardless of the type of report, IS&T issues and/or concerns will primarily be reflected in the Management component of CAMEL. Obviously, other components such as Capital and Earnings could be affected as well, however, the primary impact is on the management component. When considering the rating impact, examiners will take into account the credit union's IS&T:

- Strategic Plan & Goals and how those tie into the credit union's overall strategic plan and goals;
- Risk Analysis Process;
- Policies/Procedures/Practices; and
- Oversight Function.

Vendor IS&T Reviews

The next item I would like to discuss is Vendor IS&T Reviews. These reviews may be conducted by NCUA or one of the FFIEC agencies (Federal Reserve Board, Federal Deposit Insurance Corporation, Office of Thrift Supervision, or Office of the Comptroller of Currency). The primary difference between the two types is that NCUA uses an internally developed vendor examination program in lieu of the FFIEC examination program (contained in the FFIEC Information Systems Examination Handbook). By the

way, the handbook is an excellent source of material and information. It is available for download from our website for free, or you may order a copy (2 volumes) from our Publications Department for \$50 (Please note: quantities are extremely limited). One final word on the handbook is that the FFIEC agencies are working to update the examination process for changes in the IS&T environment since 1996. We hope to have a revised version available in 2001.

The NCUA program is a high-level review process designed from a risk-based perspective. The FFIEC program is a risk-based, thorough, and in-depth examination of a vendor's information systems, processes (including systems design, development, testing, and implementation), and business continuity and disaster recovery plans. In both types, the lead agency will provide a report of examination to the vendor, and in most cases, the regulated financial institutions of that vendor will receive a copy of the report from their regulator (not from the vendor).

Security Issues

Our final discussion area today is security...it's a small word with major implications and ramifications. In the context of this presentation, we cannot possibly even begin to scratch the surface of this issue; therefore, I will discuss it at an extremely high level. Over and over again we (NCUA) are asked how much security must a credit union employ...generally, my response is as much as you believe you need to protect the assets of your credit union and to protect your member interests'. There is no true answer to that question that can satisfy any inquirer...each credit union operates in its own unique environment which can, and generally does, change frequently. What you may consider secured and protected one day may be considered vulnerable the next day due to a change in your internal environment or a change in your external environment. When struggling with the security issue, credit unions should keep in mind the following:

- types of hardware systems utilized;
- types of software systems utilized;

- hardware and software version levels;
- the impact of the interconnectivity of the various hardware and software systems;
 - changing a configuration (hardware or software) can have a cascade effect on downstream or upstream systems (i.e. creating a vulnerability)
- types and severity of risks imposed based upon the types of hardware and software systems in place;
- acceptable risk levels;
- criticality of systems to the credit union's operation;
 - actual criticality
 - perceived criticality (generally this is from the public perspective...i.e. reputation impact)
- cost vs. benefit of security systems (Note: Generally, the cost of an actual intrusion is much more than the cost of installing security systems);
- types of intrusion response systems employed;
 - real time vs. non-real time
 - response times associated with those systems
 - monitoring capability those systems provide
- etc...the list can go on and on.

So how should a credit union address the security issue. Through a well thought out and planned security program. The program needs to be:

- in writing and sufficiently detailed for the services and systems the credit union employs;
- approved by the board of directors and have the support of senior management; and
- effective and adequate to detect and respond to a security violation in a timely manner.

In general terms, each credit union must establish appropriate standards relating to the administrative, technical, and physical safeguards for member records and information. These safeguards are to: (1) insure the security and confidentiality of member records

and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any member.

Again, thank you for the opportunity to spend some time discussing NCUA's Information Systems & Technology initiatives. I hope that you got something useful out of this discussion.

Appendix

